AFFIDAVIT IN SUPPORT OF CIVIL FORFEITURE

I, Shauna Rust, a Special Agent with the United States Secret Service, having been duly sworn state the following:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the United States Secret Service (USSS) and have been so employed since February 2021. During the course of my career, I have been trained to conduct criminal investigations involving or relating to the financial infrastructure of the United States including financial fraud and computer crimes. I have successfully completed the Criminal Investigator Training Program at the Federal Law Enforcement Training Center (FLETC). While at FLETC, I completed blocks of instruction that enable me to identify potential sources of electronic evidence, including but not limited to computers, cell phones, and other digital storage media and to preserve and utilize such evidence. I received additional training in the Special Agent Training Course at the USSS James J. Rowley Training Center in conducting investigations into a variety of criminal violations to include fraud schemes, computer crimes, and cryptocurrency investigations. As a part of this training, I also successfully completed the USSS "Basic Investigations of Computer and Electronic Crimes." I received more computer crimes training in April 2022 when I successfully completed USSS "Network Intrusion Response" training. In August 2023, I completed an additional seven weeks of "Basic Computer Evidence Recovery Training" provided by the United States Department of Treasury and became a certified digital forensics examiner for the Secret Service. I am currently assigned to the Oklahoma City Field Office. Pursuant to my duties as a Special Agent, I have participated in and directed numerous investigations involving financial fraud and computer crimes. Based on my training and

experience, I am familiar with the tactics, methods, and techniques of committing various types of fraud in violation of federal law.

2. The information set forth in this Affidavit is based on my personal knowledge and information received from other law enforcement personnel assisting in this investigation, and through financial information, interviews, and other documents and sources. I have reviewed the information contained in this Affidavit and allege the facts contained herein to be accurate. Because this Affidavit is being submitted for the limited purpose of establishing probable cause with respect to asset forfeiture, I have not included each and every fact known to me concerning this investigation.

3. Affiant submits this Affidavit in support of a Complaint of Forfeiture *in Rem* for the following personal property:

a. contents of OKX Exchange account with User ID XXXXXXXXXXXXXX2944 totaling 12,620 USDT, which was seized on or about December 15, 2023, pursuant to a warrant issued by United States Magistrate Judge D. Edward Snow for the Eastern District of Oklahoma (23-MJ-324-DES) and delivered to the United States Secret Service on or about May 16, 2024, more completely described herein as property traceable to proceeds of violations of Title 18, United States Code, Sections 1343 and 1349, or property involved in or traceable to violations of Title 18, United States Code, Sections 1956 and/or 1957, and subject to forfeiture to the United States under Title 18, United States Code, Sections 981(a)(1)(A) and 981(a)(1)(C).

DEFINITIONS

4. "Cryptocurrencies" or "virtual currencies" or simply "crypto" are digital currencies in which transactions are verified and records maintained by a decentralized system using cryptography, rather than by a centralized authority. Cryptocurrencies can be digitally traded and

function as a medium of exchange, a unit of account, and a store of value. Unlike fiat currency (which derives its value from government regulation or law; ex.: U.S. dollar), virtual currency is neither issued nor guaranteed by any government, bank, or company, but rather is generated and controlled through computer software.

5. Bitcoin" is a decentralized cryptocurrency that uses an internet-based infrastructure of nodes to store a public ledger of transactions. Bitcoin is often used by cybercriminals to conduct transactions because it operates internationally and there are various bitcoin exchangers that will convert bitcoin to fiat currency for cybercriminals.

6. "Ether" is another type of decentralized cryptocurrency that uses an internet-based infrastructure.

7. "Blockchain" is a system in which a record of cryptocurrency transactions is maintained across a large network of computers. This is essentially a distributed public ledger that keeps track of all transactions for a given cryptocurrency, incoming and outgoing, and updates regularly (multiple times per hour). The blockchain records every address that has ever received a unit of that cryptocurrency and maintains records of every transaction for each public address. This is true for Bitcoin on the Bitcoin blockchain, and for Ether on the Ethereum blockchain. The integrity of the historical record on a blockchain is secured using cryptography.

8. "Ethereum" is the name of the blockchain platform where the cryptocurrency "Ether" is used.

9. Bitcoin and Ethereum are just two forms of cryptocurrency, and there are a significant number of other varieties. When a user acquires cryptocurrency, ownership of the cryptocurrency is transferred to the user's "public address" on the blockchain for that cryptocurrency. The "public address" is somewhat analogous to a bank account number and is

comprised of a string of letters and numbers that is often dozens of characters in length (depending on the cryptocurrency). All transactions for Bitcoin, Ether, and many other cryptocurrencies are recorded on a blockchain.

10. Little to no personally identifiable information about the payer or payee is transmitted in a transaction on the Bitcoin or Ethereum blockchains. These transactions occur using a public key and a private key. A public key (reflected in the public address) is used to receive units of the cryptocurrency, and a private key is used to make withdrawals from a public address. This is done by using the private key in a cryptographic "digital signature" that provides for verification and non-repudiation, in that only a person or entity holding the private key corresponding to a given public address (public key) can provide a verifiable digital signature, and anyone in the Bitcoin or Ethereum network can use that digital signature to authenticate the transaction. Only the public address of the receiving party and the sender's private key are needed to complete the transaction, which by themselves rarely reflect any identifying information.

11. Digital currencies, including Bitcoin and Ether, have many known legitimate uses. However, much like cash, these cryptocurrencies can be used to facilitate illicit transactions and to launder criminal proceeds, given the ease with which they can be used to move funds with high levels of anonymity.

12. "Tether," or "USDT," is what is known as a "Stablecoin." Tether is a cryptocurrency designed to provide a stable price point. Tether was created by Tether Limited to function as a "digital dollar" with a stable price equivalent to U.S. Dollars and backed by physical reserves.

13. "Cryptocurrency Wallets" are pieces of hardware or software that contain a set of cryptocurrency addresses and their corresponding private keys, which can be used to transfer funds

from those addresses. The term "wallet" is also used to refer to an address or a collection of addresses that are controlled by the same entity.

14. As described above, ownership of cryptocurrency is established through the record of transfers between public addresses on a blockchain. Private keys are used to control the transfer of assets from those addresses. "Hardware wallets" are electronic storage devices, often the approximate size of a USB storage device commonly known as a "thumb drive," that store private keys in encrypted form. They are typically protected by a passcode or PIN that is needed to decipher the contents and utilize private keys to send cryptocurrency associated with the corresponding set of public addresses. Access to a hardware wallet along with the passcode or PIN enables a user to transfer funds out of those addresses into other addresses.

15. "Cryptocurrency Exchanges" are businesses that facilitate the conversion of cryptocurrency to cash or another type of cryptocurrency. An exchange typically accepts payments of fiat currency or other cryptocurrencies to obtain the desired cryptocurrency. When a user wishes to purchase, for example, bitcoins from an exchanger, the user will typically send payment in the form of fiat currency, often via bank wire or ACH, or other digital currency, to an exchanger for the corresponding number of bitcoins based on a fluctuating exchange rate. The exchanger, often for a commission, will then typically attempt to broker the purchase with another user of the exchange that is trying to sell bitcoins, or, in some instances, will act as the seller itself. If the exchanger can place a buyer with a seller, then the transaction can be completed. The user can then conduct transactions with other users of the cryptocurrency, by transferring bitcoins to their Bitcoin addresses, via the Internet.

16. "Hot Wallets" are cryptocurrency wallets used by an exchange as a systematic intermediary between customer transactions. Hot wallets are used to process users' deposits and withdrawals.

17. "OKX" is a cryptocurrency exchange service based in The Seychelles.

18. "Aux Cates FinTech Co., Ltd." is the service provider for OKX.

19. "WhatsApp" is an instant messaging service. WhatsApp can be used on a computer or downloaded as an application to a cell phone. WhatsApp provides fully encrypted messaging, file sharing, and voice or video calling.

20. "Telegram Messenger" or simply "Telegram" is an instant messaging service. Telegram can be used on a computer or downloaded as an application to a cell phone. Telegram provided fully encrypted messaging, file sharing, and voice or video calling.

21. "Pig Butchering" is the name of an investment scam becoming extremely prevalent in the United States. Pig Butchering originated in China in 2019. The scheme often begins with a scammer sending a victim a seemingly misdialed text message, communication on a dating app, or message on an instant messaging service. From there, the scammer establishes a more personal relationship with the victim using manipulative, social engineering tactics like those used in online romance scams.

22. The victims in Pig Butchering scams are referred to as "pigs" by the scammers, because the scammers will use elaborate storylines to "fatten up" victims. Once the victim reaches a certain point of trust, they are told about a cryptocurrency investment project and provided fabricated evidence to bolster the scheme's legitimacy and reduce any skepticism the victim may have in the scam. The fabricated evidence often includes a fake investment platform via a website or mobile application that displays fictitious investment gains. In reality, the website or application

has limited functionality and does not provide the user any access to a cryptocurrency wallet. The scammer may even show fake transaction photos that create the impression the victim is earning interest on their "investment." However, the investment gains displayed on the platform are fabricated. In actuality, the platform does not exist. When the victims attempt to withdraw, or "cash out," their funds the scammers will then refer to "butchering" the victim by stealing the victim's funds and refusing the return any of the money. Pig Butchering can cause very high-dollar losses and emotional distress for victims.

STATEMENT OF PROBABLE CAUSE

23. On April 20, 2023, A.Y. contacted the USSS Oklahoma City Field Office to report she had been the victim of a cryptocurrency investment scam (also known as Pig Butchering). A.Y. lives within the Eastern District of Oklahoma and stated she lost more than $700,000 to the scam. A.Y. was added to five (5) different "crypto investment" groups on Telegram and WhatsApp in September and October 2022. Multiple individuals in these group chats posed as cryptocurrency investment experts and sent A.Y. messages convincing her send approximately twenty (20) individual transactions of cryptocurrency to different fraudulent crypto wallets from September 2022 to April 2023.

24. A.Y. believed she was sending the funds to the below-listed investment platforms and individuals:

a. "gaussiancoin.com" per the instructions of an individual claiming to be "Michael Hewson CMC Analyst."

b. "Mr. Donald" and "Monica" on Telegram.

c. "Willie Investment Team."

d. "bn93.com" per the instructions of "VR_Rose1."

e. "Blackrock" investment group.

25. Affiant reviewed messages between suspects and A.Y. on Telegram. The messages showed suspects claiming A.Y. was being recruited into a training class for cryptocurrency trading with profits of over 100,000 USDT. A.Y. initially stated she was not interested. The suspects further stated A.Y. would receive various amounts of monetary "rewards" for sending Tether to them. The suspects continued to message A.Y. for several days, including a message stating "Senior Assistant Sieman" would invite A.Y. to a messaging group for guidance in investing in cryptocurrency. After these messages, and multiple others like them convincing A.Y. to send cryptocurrency, A.Y. sent her first transaction along with the message "Hoping this is safe and right decision to invest in this." Suspects responded to A.Y., telling her she would "definitely get stable high income!"

26. A.Y. told investigators after she made over twenty (20) transactions, she was told her money was out earning the stock market by a wide margin and she had a profit of three million dollars. A.Y. said when she asked to withdraw some of her earnings, suspects told her she had to pay tens of thousands of dollars in additional cryptocurrency for fees. When she asked one time about withdrawing, she was told she had to pay thirty thousand (30,000) in Tether for the "exchange function." Another time she asked to withdraw her funds, she was told she needed to pay fifteen (15) percent of the amount she was withdrawing. Another time she asked to withdraw her funds, she was told she had to pay a "20% tax (40k)" in order to withdraw her funds. A.Y. stated she could not pay the additional fees demanded for withdrawing her funds and then suspects stopped reaching out to her. A.Y. told investigators once she could not withdraw any of her funds, she realized the investment was a scam.

27. Affiant has learned through training and experience there are many different types of wire fraud schemes such as romance scams, lottery scams, Social Security scams, and Pig Butchering scams, among others. Wire fraud schemes rely on unsuspecting victims to utilize various types of financial accounts in order to conduct financial transactions that facilitate the fraud schemes. Depending on the "fraud story," the victims are led to believe they need to send money in order to receive a larger sum of money or other form of benefit. Often, the initial transactions are in small amounts and are designed to gain the victim's trust. The goal of these wire fraud schemes, described herein, is to steal money from the victims through fraud and deceit.

28. A.Y. sent her funds directly to an address controlled by one group of suspects and not any legitimate investment platform. None of the individuals are likely the person they pretended to be and are in fact played by more than one person. In Pig Butchering schemes, it is common for multiple, low-level members of a criminal organization to pretend to be a single person when communicating with a victim. When A.Y. attempted to withdraw her funds, she realized she had been scammed.

29. This investigation revealed the controller of the Target Account also utilized private addresses for the token movements which is indicative of money laundering tactics used to conceal and disguise the source of originating victim funds. Private wallets are non-custodial wallets, meaning an owner, as opposed to a host exchange, such as OKX, controls the private keys and therefore all associated funding without oversight or financial regulation. Private, non-custodial wallets can be held in numerous forms such as wallet applications on computers and cell phones or cold storage devices not connected to the internet. In this case, some of the victim's funds were transferred to private wallet addresses and some were sent to the host exchange wallets, including the Target Account – a wallet hosted by the OKX exchange.

30. Review of the blockchain and available records indicates the proceeds from this scam were laundered through numerous cryptocurrency addresses.

Movement of Victims Funds to Target Account

31. In summary, A.Y. sent a total of $176,901 in digital currency to wallets controlled by the OKX in three (3) transactions. Each of these transactions were laundered through numerous different cryptocurrency exchanges, wallets, and changed from Ethereum to Tether (USDT) before arriving in the listed OKX wallet. There is no apparent reason, economic or otherwise, for the use of such a complex movement of cryptocurrency through the use of multiple intermediary wallet addresses, unless the purpose is to conceal the nature, source, location, ownership or control of the funds at issue. The transactions were processed by OKX hot wallets and then deposited in two suspect accounts, including the Target Account. Once within the Target Account, victim funds were co-mingled with other funds. Affiant recognizes through training and experience these to be steps taken by suspects to further obfuscate and launder illicit proceeds. The details of the three (3) victim transactions are listed below:

a. October 21, 2022

i. Amount: $488

ii. OKX Destination: 0x96fdc631f02207b72e5804428dee274cf2ac0bcd (OKX Hot Wallet, used for processing)

b. November 9th, 2022

i. Amount: $94,795

ii. OKX Destination: 0x9723b6d608d4841eb4ab131687a5d4764eb30138 (OKX Hot Wallet, used for processing)

iii. OKX Destination: 0x68841a1806ff291314946eebd0cda8b348e73d6d

(OKX Hot Wallet, used for processing)

iv. OKX Destination: 0x23958fb01c9c60c188689c13711bae0b72f6ed84 Target Account)

c. November 15, 2022

i. Amount: $76,616

ii. Destination: 0x68841a1806ff291314946eebd0cda8b348e73d6d (OKX hot wallet used for processing)

iii. Destination: 0x276cdba3a39abf9cedba0f1948312c06 (unidentified wallet)

iv. Destination: 0x89c619749b680fe6659ba2cdc6caa8a612c051e0 (additional suspect account, no remaining balance)

OKX Records

32. On June 8, 2023, Affiant sent a request on USSS letterhead to the OKX exchange for account details and transaction history for the Target Account. Later the same day, OKX provided the requested records, summarized below:

a. User ID: XXXXXXXXXXXXXX2944

b. Wallet: 0x23958fb01c9c60c188689c13711bae0b72f6ed84

c. Balance: 29,847.20 Tether

d. Username: 练子营 (Google Translate translation: Liàn zi yíng)

33. The records also included a People's Republic of China identification card with a photo of an adult male. The balance of the account was made up of dozens of different forms of cryptocurrency with a value of 29,847.20 in Tether, equivalent to $29,847.20. The deposit history shows approximately two-hundred and fifty (250) deposits into the Target Account between

January and November 2022. The large volume of deposits in a short period of time is an indicator of fraudulent activity common with cryptocurrency wallets involved in Pig Butchering scams.

34. On June 13, 2023, Affiant sent a request on USSS letterhead to OKX to freeze the funds in the Target Account. OKX acknowledged this request and informed investigators they would freeze the funds in the suspect's account and could transfer the victim's funds to a USSS cryptocurrency wallet once provided with a court order. OKX was provided with a seizure warrant from the Eastern District of Oklahoma on December 15, 2023, for the 29,847.20 Tether in the suspect's wallet. On May 16, 2024, OKX transferred 12,620 Tether to the U.S. Secret Service Oklahoma City Field Office cryptocurrency wallet. Investigators attempted additional contact with OKX to determine the status of the remaining balance from the 29,847.20 Tether located in the suspect's account and did not receive any response.

CONCLUSION

35. Affiant submits there is probable cause to believe the contents of OKX Exchange account with User ID XXXXXXXXXXXXXX2944 totaling 12,620 USDT, seized pursuant to a warrant issued by the United States District Court for the Eastern District of Oklahoma, as described above, constitute or were derived from proceeds traceable to Wire Fraud, in violation of 18 U.S.C. §1343, Conspiracy to Commit Wire Fraud, in violation of 18 U.S.C. §1349, and/or property involved in Money Laundering, in violation of 18 U.S.C. §§ 1956 and 1957.

36. Title 18, U.S.C. § 981(a)(1)(C) provides for the civil forfeiture of any proceeds constituting or derived from, proceeds traceable to any offense defined as a "specified unlawful activity" as defined in 18 U.S.C. § 1956(c)(7), which includes violations of 18 U.S.C. § 1343 as listed in 18 U.S.C. § 1961.

37. Further, 18 U.S.C. § 981(a)(1)(A) provides for the civil forfeiture of any property involved in a transaction or attempted transaction in violation of 18 U.S.C. §§ 1956 or 1957, or any property traceable to such property.

38. Therefore, the contents seized from OKX Exchange account with User ID XXXXXXXXXXXXX2944 totaling 12,620 USDT are subject to seizure pursuant to 18 U.S.C. § 981(b), and forfeiture to the United States pursuant to 18 U.S.C. §§ 981(a)(1)(A) and 981(a)(1)(C).

39. Pursuant to 18 U.S.C.§ 981(b)(3), a seizure warrant may be issued in any district in which a forfeiture action against the property may be filed under 28 U.S.C. § 1355(b) and executed in any district in which the property is found or transmitted to the central authority of any foreign state for service in accordance with any treaty or other international agreement.

I, Shauna Rust, a Special Agent with the United States Secret Service, being duly sworn according to law, hereby state that the facts stated in the foregoing affidavit are true and correct to the best of my knowledge, information, and belief.

SHAUNA RUST, Special Agent
United States Secret Service

STATE OF OKLAHOMA)
) ss
COUNTY OF OKLAHOMA)

Be it remembered, that on this 13th day of September 2024, before me a notary public in and for said State, personally appeared Shauna Rust to me known to be the identical person described in and who executed the within and foregoing instrument and acknowledged to me that he executed the same as his free and voluntary act and deed for the uses and purposes therein set forth.

In witness whereof, I have hereunto set my official signature and affixed my notarial seal, the day and year first above written.

WILLIAM ALVA WIND
Notary Public, State of Oklahoma
Commission # 20004947
My Commission Expires 05-06-2028

NOTARY PUBLIC

Commission Number: 20004947

My Commission Expires: MAY 6, 2028